Fig.1

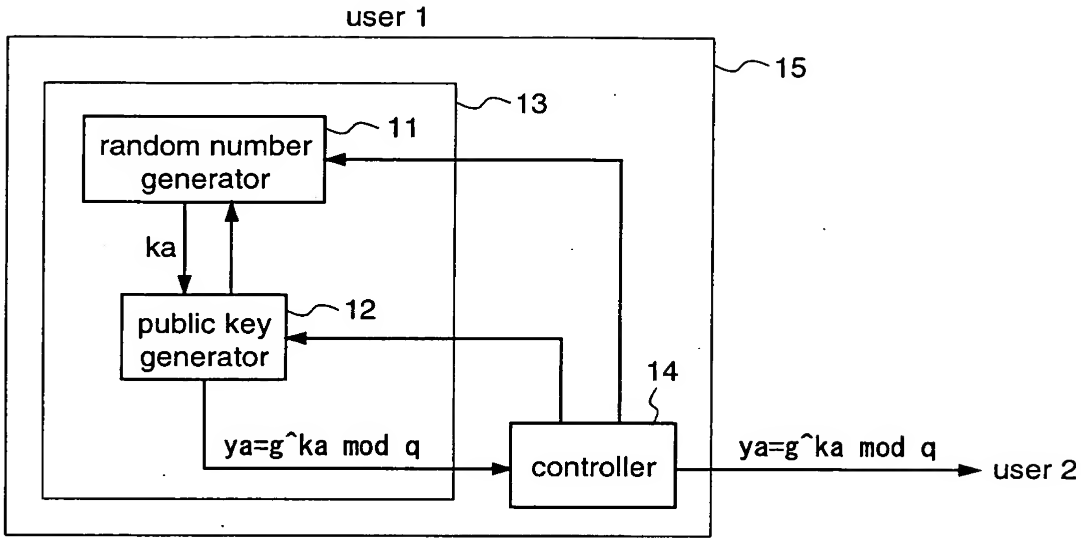

user 1
15
13
random number generator
11
ka
public key generator
12
14
ya=g^ka mod q
controller
ya=g^ka mod q
user 2

Fig.2

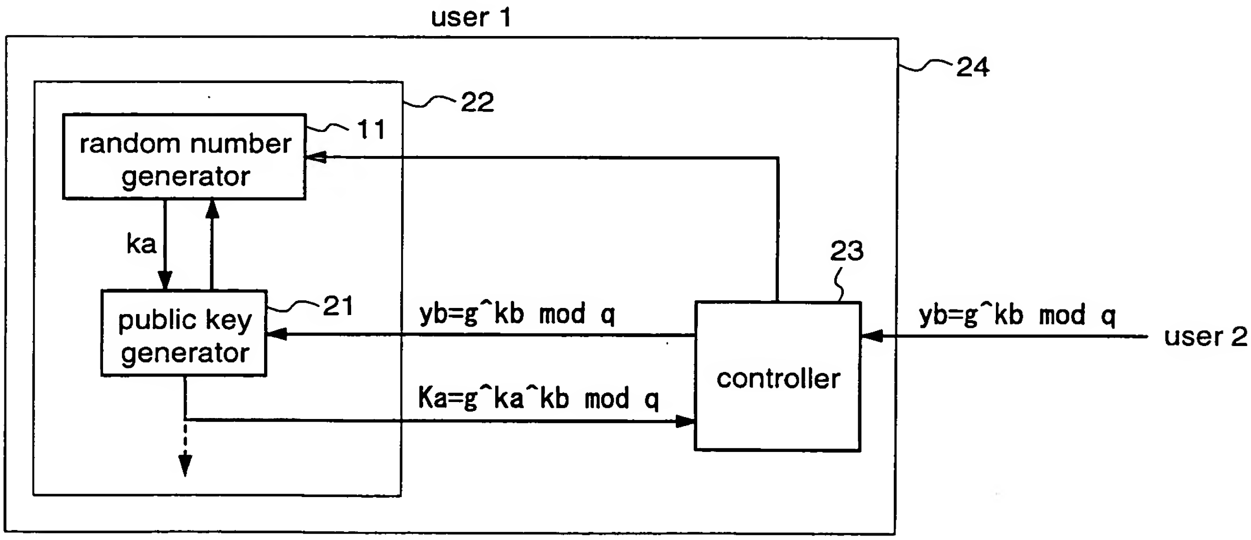

user 1
24
22
random number generator
11
ka
23
public key generator
21
yb=g^kb mod q
yb=g^kb mod q
user 2
controller
Ka=g^ka^kb mod q

Fig.3

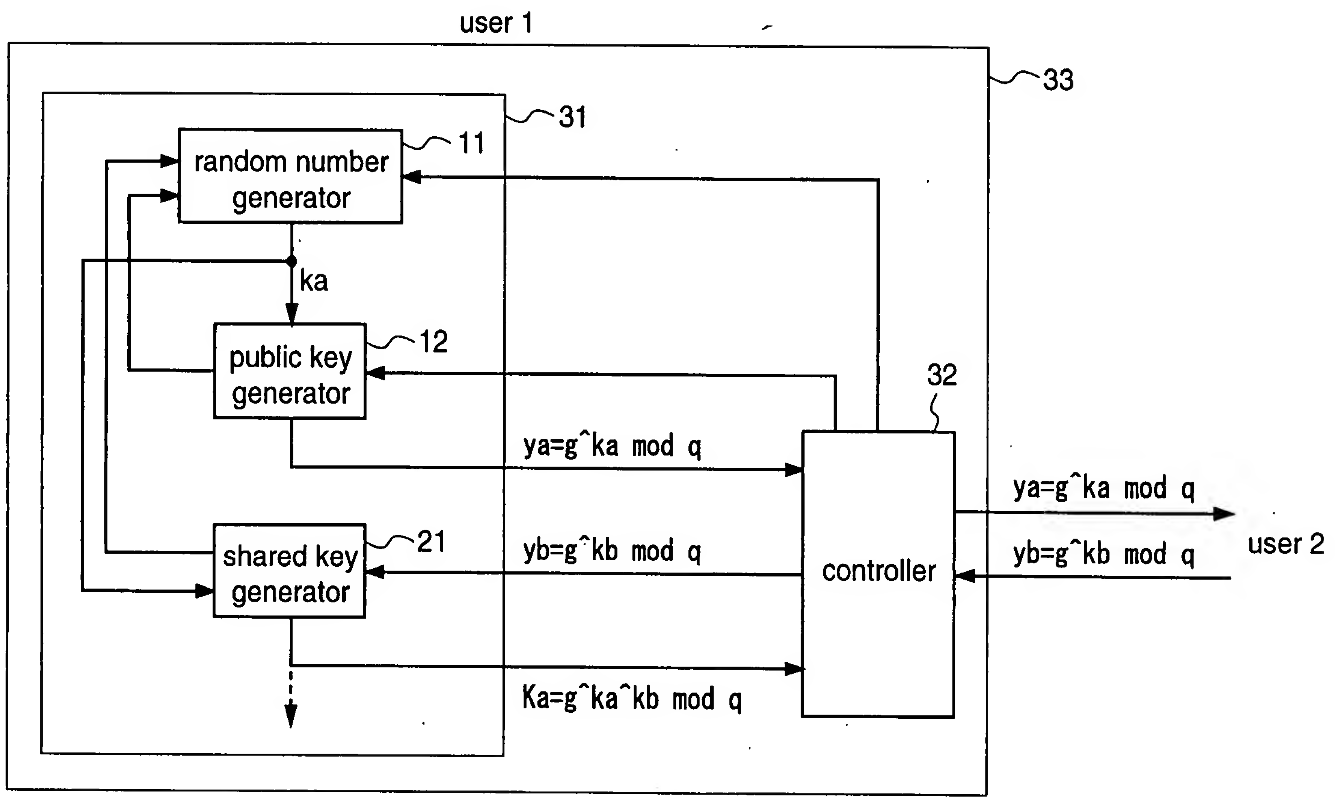

user 1
33
31
random number generator
11
ka
public key generator
12
32
ya=g^ka mod q
ya=g^ka mod q
shared key generator
21
yb=g^kb mod q
controller
yb=g^kb mod q
user 2
Ka=g^ka^kb mod q

Fig.4

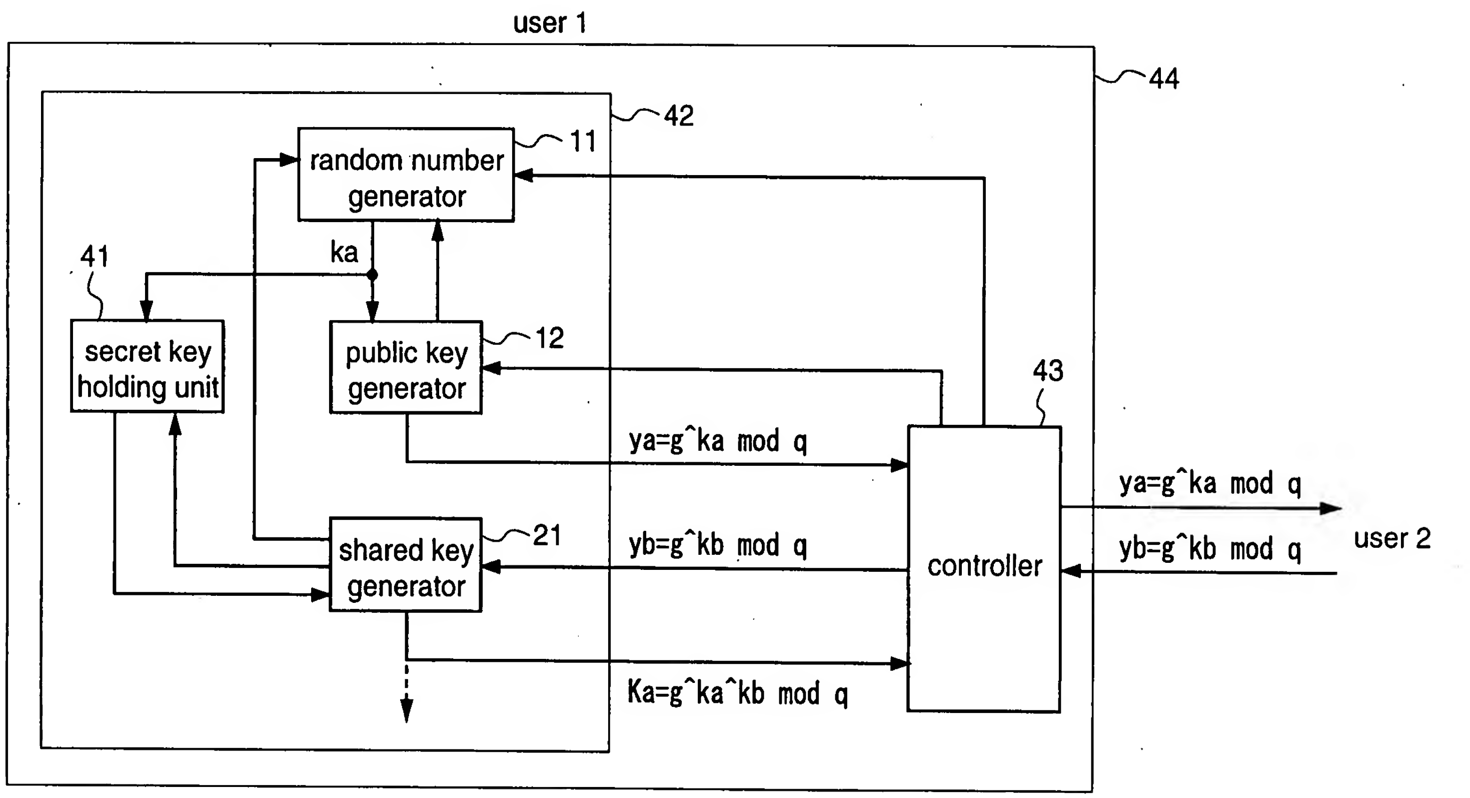
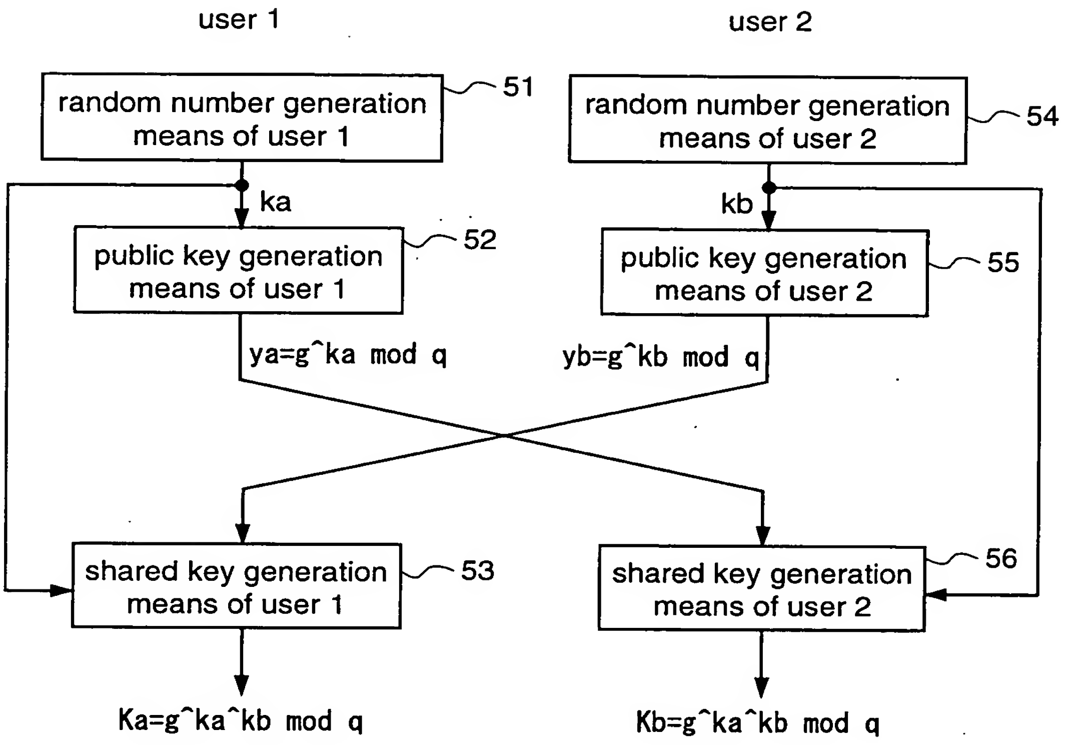

user 1
44
42
random number generator
11
ka
41
secret key holding unit
public key generator
12
43
ya=g^ka mod q
shared key generator
21
yb=g^kb mod q
controller
ya=g^ka mod q
yb=g^kb mod q
user 2
Ka=g^ka^kb mod q

Fig.5 Prior Art


user 1
user 2
random number generation means of user 1
51
random number generation means of user 2
54
ka
kb
public key generation means of user 1
52
public key generation means of user 2
55
ya=g^ka mod q
yb=g^kb mod q
shared key generation means of user 1
53
shared key generation means of user 2
56
Ka=g^ka^kb mod q
Kb=g^ka^kb mod q